Wertkonflikte in einem «sicheren» digitalen Gesundheitssystem

Christen, Markus

Wertkonflikte in einem «sicheren» digitalen Gesundheitssystem [1]

VON DR. SC. ETH MARKUS CHRISTEN
GESCHÄFTSFÜHRER DER «DIGITAL SOCIETY INITIATIVE» DER UNIVERSITÄT ZÜRICH

Ein digitales Gesundheitswesen stellt Fragen, die über den reinen Datenschutz hinausgehen. Weil digitale Bedrohungen das Funktionieren des ganzen Gesundheitssystems beeinträchtigen können, hat sich die Informationssicherheit zu einem zentralen Erfordernis entwickelt. Im Bereich des Gesundheitswesens gehen damit aber schwierig zu lösende Wertkonflikte einher.

Intensive Nachforschungen haben bei den Spezialisten des staatlichen «Computer Emergency Response Team» (CERT) endlich zum erwünschten Erfolg geführt: Man hat einen zentralen Knotenrechner eines «Bot-Netzes» identifiziert – eines Netzes von Tausenden von Computern, die heimlich gehackt worden sind und nun im Dienst von Kriminellen beispielsweise für Erpressungsangriffe gegen Internet-Server genutzt werden, ohne dass die Besitzer der Computer irgendwas davon wissen. Kurz bevor die Experten des CERT den gehackten Rechner «killten» – ihn also ferngesteuert ausschalteten, um damit das Botnet zu zerstören –, erfolgte eine letzte Prüfung, wo denn dieser Rechner steht. Die IP-Adresse verweist auf ein Universitätsspital, und Nachforschungen zeigen: Es ist kein «normaler» Computer; es handelt sich um eine Herz-Lungen-Maschine, angeschlossen an das Internet, damit man sie einfacher bedienen kann. Hätte man sie «gekillt», wäre aus der metaphorischen Verwendung dieses Wortes eine buchstäbliche geworden.

Ungenügend geschütztes Gesundheitssystem

Beispiele dieser Art verlassen selten die informellen Sphären hochspezialisierter Experten. Doch auch die Öffentlichkeit vernahm in den letzten Jahren eine Häufung von Meldungen von Cyber-Angriffen auf Spitäler. Jüngste globale Angriffe wie WannaCry im Mai 2017 – ein sogenannter «Verschlüsselungs-Troianer», der Informationen auf einem Rechner unzugänglich macht, womit die Betroffenen dann erpresst werden – hatten erhebliche Auswirkungen auf die digitale Infrastruktur vieler Anbieter im Gesundheitswesen. Sie zeigten, dass die Cyber-Sicherheit in diesem Bereich im Vergleich beispielsweise zum Finanzsektor unterentwickelt ist. Warum ist das so, wenn doch Gesundheit ein zentraler Wert für Menschen ist und Gesundheitsdaten sehr sensibel sind?

Ein wichtiger Grund dafür ist, dass der Wert der «Sicherheit» (bzw. Cybersecurity) mit anderen wichtigen Werten des Gesundheitssystems in einem komplexen Spannungsverhältnis steht. Nehmen wir das Beispiel der Autonomie: Beim Einsatz von Informations- und Kommunikationstechnologie (IKT) im Gesundheitswesen soll sichergestellt werden, dass die Patienten selbst bestimmen, welche Informationen an wen weitergegeben werden – beispielhaft dafür ist das neue elektronische Patientendossier in der Schweiz. Würde der Schutz aber überbetont, kann dies dazu führen, dass in Notfällen wichtige medizinische Informationen – beispielsweise über Allergien gegen bestimmte Medikamente – nicht zugänglich sind. Hier stellt sich das Problem des Umgangs mit fehlender Entscheidungsfähigkeit des Patienten in neuer Form.

Ansprüche an IKT im Gesundheitswesen

Es ist heute unbestritten, dass die Nutzung von IKT im Gesundheitswesen zahlreiche Vorteile hat. Fast alle modernen Geräte für Diagnose und Therapie beruhen massgebend auf digitaler Technologie. Kein Spital wird heute auf die Nutzung von IKT für die Verwaltung von Gesundheitsinformationen verzichten. All dies geschieht mit dem Wunsch einer sachgerechten Anwendung, was vier Ansprüche umfasst. So sollen erstens die IKT-Systeme zu einer Verbesserung von Effizienz und Qualität des Gesundheitssystems führen. Zweitens sollen sensible Informationen und vertrauliche Kommunikation geschützt werden, um so die Privatsphäre der involvierten Personen zu wahren. Drittens sollen die Systeme einfach bedient werden können, d. h., die sogenannte «Usability» soll hoch sein. Viertens soll die Nutzung der Systeme die Patientensicherheit nicht gefährden.

Bei all diesen Ansprüchen spielt Cybersecurity eine wichtige Rolle. Gemäss einer generellen Definition durch die Internationale Fernmeldeunion ist damit die Gesamtheit von Tools, Policies, Sicherheitskonzepten, Richtlinien, Schulungen etc. gemeint, mit dem Ziel, die Cyber-Ressourcen einer Organisation (Daten, Computer, Software, Kommunikationseinrichtungen etc.) zu schützen. Die allgemeinen Sicherheitsziele umfassen Verfügbarkeit, Integrität und Vertraulichkeit von Systemen und Daten

Im Gesundheitssystem sind drei Arten von Bedrohungen relevant: Bedrohungen gegen Informationen, gegen Informationssysteme und gegen medizinische Geräte bzw. Implantate.

Prinzipien als Orientierungspunkte

Wie kann nun das Erfordernis von Cybersecurity Wertkonflikte hervorrufen? Um diese Frage zu beantworten, eignen sich die in der Medizin wohlbekannten vier Prinzipien der biomedizinischen Ethik als Orientierungspunkt. Die Definition dieser von Tom Lamar Beauchamp und James F. Childress vorgeschlagenen Prinzipien lässt sich wie folgt zusammenfassen:

- Respekt vor der Autonomie bedeutet das Recht des Einzelnen (Patienten), seine eigene Wahl zu treffen, insbesondere in Bezug auf medizinische Entscheidungen. Er beinhaltet das Recht, in geeigneter Weise über therapeutische und diagnostische Möglichkeiten informiert zu werden.
- Das Prinzip des Nichtschadens lässt sich aus dem klassischen Zitat «primum non nocere» des hippokratischen Eids herleiten. Es umfasst die Pflicht, Risiko-Nutzen-Bewertungen vorzunehmen und Risiken für Patienten (und andere) aufgrund medizinischer Massnahmen (oder Unterlassungen) zu minimieren.
- Das Prinzip der Fürsorge verlangt, dass man im besten Interesse des anderen handelt. Es spiegelt die grundlegende moralische Motivation des medizinischen Handelns wider, nämlich den Gesundheitszustand und die Lebensqualität von Patienten zu verbessern.
- Das Prinzip der Gerechtigkeit betont Fairness und Gleichheit unter den Menschen. Es erfordert, einen ganzheitlichen Blickwinkel einzunehmen, beispielsweise unter dem Aspekt der Verteilungsgerechtigkeit knapper Güter.

Die genannten Anforderungen an die Nutzung von IKT im Gesundheitswesen

widerspiegeln diese Prinzipien, wie nachfolgend vereinfacht skizziert wird: Qualität und Effizienz haben einen Bezug zur Fürsorge: Ein kostengünstigeres System kann potenziell mehr Menschen unterstützen. Qualitätsverbesserungen können Menschen helfen, denen in der Vergangenheit nicht geholfen werden konnte. Privatsphäre und Vertraulichkeit gründen in Autonomie und Nichtschaden, weil Personen über ihre sensiblen Informationen selbst bestimmen wollen und Verletzungen von Vertraulichkeit z. B. zu Diskriminierung führen können. «Usability» hat primär einen Bezug zu Gerechtigkeit, aber auch zu Nichtschaden und Autonomie. Tiefe «Usability» digitaler Systeme kann Personen mit wenig IKT-Erfahrung von der Nutzung bestimmter Services ausschliessen. Patientensicherheit schliesslich hat vorab mit dem Prinzip des Nichtschadens zu tun.

Wie in anderen Bereichen der Medizinethik können auch in dem der Cybersecurity diese Werte zueinander in Konflikt geraten, wie hier anhand weniger Beispiele gezeigt wird:

- **Fürsorge und Autonomie vs. Nichtschaden und Gerechtigkeit:** Angenommen, Cybersecurity im Gesundheitswesen ist darauf ausgerichtet, die Qualität und Effizienz der Dienste sowie die Vertraulichkeit von Informationen und die Vertraulichkeit der Kommunikation zu optimieren. Solche Systeme sind oft sehr komplex und schwer zu bedienen – Letzteres bedeutet oft eine Zugangsschwelle für die, denen die entsprechenden Kompetenzen fehlen. Kryptografisch gut geschützte Implantate können die Benutzerfreundlichkeit in kritischen Situationen beeinträchtigen und die Batterielebensdauer verringern, was mit dem Prinzip des Nichtschadens in Konflikt steht.
- **Nichtschaden, Fürsorge und Gerechtigkeit vs. Autonomie:** Nehmen wir an, dass die Qualität und Effizienz der Dienste optimiert werden, zusammen mit der Benutzerfreundlichkeit, wobei aber die Privatsphäre und die Vertraulichkeit geopfert werden. Auch hier kann ein solches Design einige Aspekte des Fürsorgeprinzips (erleichterter Datenaustausch für die Forschung) und des Nichtschaden-Prinzips (Patientenüberwachung) erfüllen, es dürfte dann aber die Autonomie verletzen.
- **Nichtschaden und Autonomie vs. Fürsorge und Gerechtigkeit:** Nehmen wir an, ein System für Gesundheitsinformationen wurde optimiert, um die Privatsphäre und Sicherheit zu fördern. Ein solches System kann in der Lage sein, Datenschutzverletzungen sowie z. B. *Denial-of-Service*-Angriffe zu verhindern. Dies würde dem Grundsatz der Autonomie und des Nichtschadens Rechnung tragen. Ein solches Design könnte jedoch nicht für die Erbringung datenintensiver Dienste verwendet werden, was im Widerspruch zum Grundsatz der Fürsorge stehen sowie einen Verlust an Qualität und/oder Kosteneffizienz bedeuten kann – Letzteres eine Forderung der Gerechtigkeit.

Diese kurze Zusammenstellung zeigt: Die Ansprüche an ein sicheres digitales Gesundheitswesen tragen Wertkonflikte in sich, die nicht einfach handhabbar sind.

In manchen Fällen könnten technische Lösungen Wertkonflikte entschärfen – beispielsweise einfachere und dennoch sichere Formen von Authentifizierung. Doch in anderen Fällen wird man um Wertabwägungen nicht herumkommen. Daher ist der Einbezug von ethischem Denken unabdingbar, um solche Wertkonflikte zu erkennen und gemeinsam tragfähige Lösungen zu entwickeln.

Über den Autor

Dr. sc. ETH Markus Christen ist Forschungsgruppenleiter am Institut für biomedizinische Ethik und Medizingeschichte der Universität Zürich und Geschäftsführer der «Digital Society Initiative» der Universität Zürich. Seine Forschungsgebiete sind Ethik von Informations- und Kommunikationssystemen, Neuroethik und empirische Ethik.

1 Dieser Artikel basiert auf einem längeren Beitrag, der im September 2018 an der Informations- und Computer-Ethik-Konferenz «Ethicomp 2018» vorgestellt wird: Michele Loi, Markus Christen, Nadine Kleine, Karsten Weber: Cybersecurity in health – disentangling value tensions